CISA
CYBER+INFRASTRUCTURE

ELECTION INFRASTRUCTURE SUBSECTOR-SPECIFIC PLAN

An Annex to the NIPP 2013

2020

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency

EXHIBIT 2

This Page is Intentionally Left Blank.

EXHIBIT 2

TABLE OF CONTENTS

EXHIBIT 2

LETTER FROM THE COUNCIL CHAIRS

The security and resilience of election infrastructure is crucial to national security. Given election infrastructure's designation as critical infrastructure, the U.S. Department of Homeland Security (DHS), as the Sector-Specific Agency, has established governance structures to collaborate across the community to ensure a unified national effort to secure elections. Most prominently, DHS has partnered with the Election Assistance Commission, other federal entities, and state and local leaders to establish an Election Infrastructure Subsector Government Coordinating Council (GCC) to guide efforts across all levels of government to secure elections. At the same time, industry representatives who support the conduct of elections have established an Election Infrastructure Subsector Coordinating Council (SCC) to partner with the government to bring joint public-private resources to bear for this crucial mission.

This Election Infrastructure Subsector-Specific Plan (SSP) is the strategic plan guiding this shared effort. Published at the beginning of 2020, it will serve as the basis by which industry and government come together to set priorities for security efforts in the face of the immediate threat to our election infrastructure, while also charting a path for ongoing collaboration and capability development in future years. The Plan identifies how key stakeholders are working together to assess and manage the Election Infrastructure Subsector risk landscape and its unique operating conditions to strengthen national security and resilience, as set forth in the [Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (PPD-21)](#) and the [National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience (NIPP 2013)](#).

2019 Sector-Specific Plan Update

The GCC and SCC jointly crafted this version of the Election Infrastructure Subsector-Specific Plan to reflect the continued growth of the Subsector and the significant progress made since the 2018 midterm election cycle. This Plan combines the mission, goals, and priorities of its public and private sector partners to help foster ongoing collaboration. It also outlines the Subsector's strategic direction for enhancing election infrastructure security.

Since DHS issued its critical infrastructure declaration for elections in 2017, Subsector stakeholders in both the public and private sectors have taken significant steps to understand and reduce risk, improve information sharing and coordination, and strengthen resilience capabilities. This Plan is intended to inform stakeholders—including election officials, members of the Executive Branch and Legislative Branch, nongovernmental organizations (NGOs), and the general public—about ongoing efforts to protect and maintain the integrity of our democratic process against nation-state threats and natural disasters of national significance.

Key Accomplishments

Since 2017, the GCC and the SCC have made considerable progress in building the Nation's election security. Notable efforts include:

- establishment of GCC and SCC to work in partnership,
- development of the Joint Election Infrastructure SSP,
- establishment of the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) and the Information Technology Information Sharing and Analysis Center (IT-ISAC) Election Industry Special Interest Group (EI-SIG) for voluntary sharing of threat and intelligence information,
- establishment of the Election Infrastructure Subsector Clearance Program,
- execution of the "Tabletop the Vote" exercises for national preparedness,
- development and deployment of the Last Mile effort, and
- preparation and delivery of legislative communications, including briefings to Members of Congress and their staff.

These achievements clearly demonstrate progress in the development, prioritization, and implementation of effective security approaches and resilience strategies. By no means, however, do they suggest that our efforts are over. Both Councils are dedicated to continuing unified efforts to address the risks to election infrastructure consistent with this Plan. We recognize the degree to which our Nation's security depends on it and are committed to our ongoing partnership in leading the national effort.

EXHIBIT 2

EXECUTIVE SUMMARY

In January 2017, DHS established the Election Infrastructure Subsector under the Government Facilities Sector through a critical infrastructure designation for election infrastructure. The designation makes it clear both domestically and internationally that election infrastructure enjoys all the benefits and protections of critical infrastructure that the U.S. Government has to offer.[1]

DHS issued this designation for elections based on a U.S. intelligence community determination that Russia sought to interfere in the 2016 presidential election through sophisticated, cyber-enabled operations.[2] Specific to election infrastructure, later U.S. Government reporting confirmed compromise attempts by Russian military actors against county and state election offices, as well as U.S. companies supplying software and other technology for administering elections.[3] Findings indicate that, while public-facing election websites and other types of infrastructure related to the registration of voters and voter databases were widely targeted, the Office of the Director of National Intelligence (DNI) concluded that "the types of systems Russian actors targeted or compromised were not involved in vote tallying."[4]

The Subsector has established partnerships among government stakeholders at the local, state, and federal levels and between the public and private sectors, forming both a GCC and an SCC. These bodies provide a mechanism for collaboration between DHS, law enforcement, the intelligence community, and private sector partners to enhance information sharing about risks to the Nation's election systems, identify resources to help mitigate such risks, communicate best practices, address identified vulnerabilities, and enable election officials' access to classified threat information. State and local governments have engaged federal counterparts, other state agencies, and the private sector with the intent to conduct vulnerability assessments on election systems and increase focus on the cybersecurity of election systems.

The SSP complements the National Infrastructure Protection Plan (NIPP) by outlining the application of the NIPP Framework to the unique risk landscape of the Election Infrastructure Subsector. It includes plans for a collaborative process between public and private sector partners in protecting election infrastructure from all hazards and threats, including natural disasters, terrorist attacks, cyberattacks, and other large-scale disruptions. The SSP includes actions and timelines for the Subsector to cooperatively and voluntarily identify and prioritize assets, assess risk, implement protective programs, and, ultimately, measure the effectiveness of this work.

Included is an overview of how the GCC and SCC manage their responsibilities in the areas of partnership/outreach, training and education, and information sharing to ensure a secure and resilient electoral system that is prepared for national cyber emergencies. Notably, this SSP identifies collaborative approaches to navigating risks in the face of limited resources, while not altering or impeding the ability of election infrastructure partners to perform their respective responsibilities under the law.

The document is divided into four main sections, based on the NIPP 2013 Risk Management Framework and other joint Subsector priorities. A brief summary of these sections follows.

1. **Subsector Profile:** Provides a concise description of the Subsector's authorities and operating characteristics, major significant components, organizational structures, and key partners.

2. **Risk Management – Assessing and Mitigating Risk:** Assessing and Mitigating Risk: Describes the Subsector's risk management approach, including collaborative programs, activities, resources, approaches to cybersecurity, and efforts to leverage research and development (R&D).

---

[1] The January 2017 Department of Homeland Security designation defines "election infrastructure" as the following:
"*storage facilities, polling places, and centralized vote tabulations locations used to support the election process, and information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of state and local governments.*"
https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

[2] U.S. Office of the Director of National Intelligence (USODNI), *Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security*, October 7, 2016.

[3] Special Counsel Robert S. Mueller III, Report on the Investigation Into Russian Interference In The 2016 Presidential Election, March 2019, https://www.justice.gov/storage/report.pdf.

[4] U.S. Office of the Director of National Intelligence (USODNI) *Joint Intelligence Community Assessment, Assessing Russian Activities and Intentions in Recent U.S. Elections, Jan. 6, 2017.*
See also: *U.S. Senate Select Committee on Intelligence, Russian Targeting of Election Infrastructure During the 2016 Election*, May 2018.

EXHIBIT 2

3. **Vision, Mission, Goals, and Objectives:** Outlines current and future plans for the Subsector to boost collective capabilities for responding to national or large-scale incidents and building resilience across the election's ecosystem through coordinated sharing of intelligence and threat information. Additionally, lists the specific activities the GCC and SCC plan to undertake to address the Subsector's priorities.

4. **National Preparedness and Resilience Strategies:** Describes the importance of preparedness for cyber and physical disruptions to the Subsector, along with resilience efforts the Subsector must undertake to prevent, deter, and mitigate these threats.

Appendices at the end of this plan detail additional support to the major sections of this SSP, including Subsector membership, a glossary of terms, references, and detailed information on risk management.

This SSP will be periodically updated to reflect changes in national priorities, lessons learned, and Subsector composition and structure.

EXHIBIT 2

1 SUBSECTOR PROFILE

This chapter outlines the makeup of the Election Infrastructure Subsector and its operating characteristics. The section also identifies the Subsector's primary risks, interdependencies, and unique mechanisms for public-private partnership. The Election Infrastructure Subsector is a functions-based subsector with both physical assets and virtual systems and networks to enable the conduct of U.S. elections.

1.1 Subsector Definition, Authorities, Critical Functions, and Evolution

The Election Infrastructure Subsector encompasses storage facilities, polling places, and centralized vote tabulation locations used to support the election process, and information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of state and local governments. It does not address certain risk areas beyond the control of election officials and out of scope of election infrastructure, including political parties, candidates, voters, the media, and other infrastructure used on Election Day, such as electricity and telecommunications networks. This is not to say that there are not potential threats to those entities, but just to acknowledge that they are not the specific purview of the Election Infrastructure Subsector framework. The complexity of accurately defining and protecting the elections ecosystem, with its separate but often interdependent facets, is a key challenge in and of itself.

The Subsector consists of an extremely diverse range of public and private owners and operators of election infrastructure. Most election facilities are government-owned agencies or sites with open access, including polling place operations. Subsector stakeholders must balance security priorities with the need to ensure accessibility, privacy, and transparency. Assets can range from physical sites and hardware to digital operations.

In general, election infrastructure is owned and operated with minimal oversight from federal entities. However, there are a number of times in contemporary U.S. history in which the Federal Government has played a role in extending election access or voting rights protections while recognizing the clear existing constitutional limitations. Specific examples include the Civil Rights Act, the Voting Rights Act of 1965, the Uniformed and Overseas Citizens Absentee Voting Act, the Americans with Disability Act, the National Voter Registration Act (NVRA), the Help America Vote Act (HAVA), and the Military and Overseas Voter Empowerment Act of 2009.

Figure 1. Federal Laws Relevant to the Election Infrastructure Subsector

EXHIBIT 2
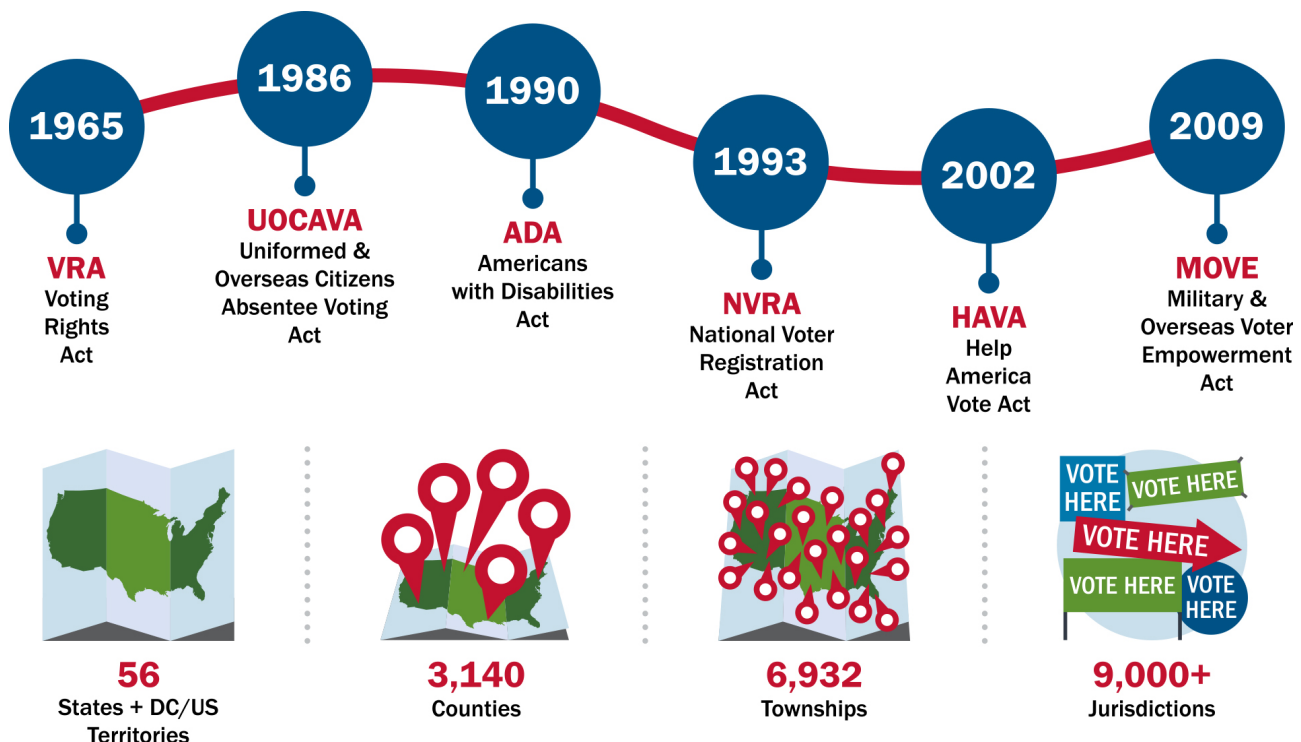
Beyond these limited exceptions, individual states and territories carry out the majority of law and policymaking around the conduct of elections. Each state and territory has a legally designated Chief Election Official charged with overseeing the conduct of elections according to law. According to the National Association of Secretaries of State (NASS), "Ensuring the integrity of the voting process is central to this role, which includes cyber preparedness and contingency planning, as well as administrative and technical support for local election officials."[5]

In some states, state-level officials play a more significant role by managing and maintaining much of the election infrastructure, including voting equipment. But nearly 9,000 local election jurisdictions carry out the rubber-meets-the-road functions of running an election at the county or municipal level. In most states, local officials select and purchase their voting systems from options approved and certified at the federal and/or state levels.

Many state and local election jurisdictions depend on third-party providers for support in conducting day-to-day management and maintenance of their election infrastructure. Industry partners are often information technology (IT)-focused companies and nonprofits, covering various types of election support, including:

- voting and election management systems;
- voter registration systems and electronic pollbooks;
- ballot programmers and printers;
- election data solutions providers;
- voter information tools and look-up features; and
- election supplies to store, transport, and use equipment.

1.1.1 Key Sector Operating Characteristics

Elections are a core facet of democratic governance. They are critical to the peaceful transition of power, requiring both the verifiable selection of winners as well as losers who can confidently accept an unfavorable outcome. Any attempt to manipulate or interfere with election infrastructure can risk undermining the right to vote, placing undue burdens on voters or impacting public confidence in the process.

Securing elections requires year-round activity. Security measures to protect election infrastructure must be implemented when technology is in use, when it is being prepared for use, and when it is not in use. Critical election infrastructure is not limited to technology that is used only during elections. It also includes technology that is in use 365 days per year, such as voter registration systems and election information websites. Further, the technology that is deployed for a specific election, such as electronic pollbooks and vote-casting and tabulation systems, is used for multiple elections per year in most jurisdictions.

Elections are highly decentralized and deadline driven. This requires active contingency planning and regional or statewide security coordination and information sharing between public and private partners. There are thousands of local election jurisdictions and hundreds of thousands of poll workers and election staff, as well as varying technology resources and types of providers. No two jurisdictions are exactly alike.

These key operating characteristics create unique scenarios for the Subsector, including those identified below:

State and local election officials are primarily responsible for protecting election infrastructure. Elections are run at the state and local levels. State and local election officials have implemented innovative measures to secure election infrastructure, often with limited resources. The Federal Government does not administer elections but has broad access to information, tools, and resources which help secure elections. Therefore, DHS and other relevant federal agencies provide important election security support to state and local governments.

Election administration is given limited resources. Many election offices face daily budget constraints and staffing shortages while managing a broad portfolio of duties. Identifying sustainable funding for managing risk in a global threat environment is an ongoing challenge, with officials often relying upon the Federal Government for resources, information sharing, and other types of support.

---

[5] National Association of Secretaries of State (NASS), "Securing Elections," January 2020, https://www.nass.org/initiatives/securing-elections.

EXHIBIT 2

State and local election officials must balance security with access and transparency. Election agencies operate on principles of open public access and transparency, which can create challenges for adopting security principles and practices. Voting sites can be soft targets due to their open access and limited security barriers, and Election Day workers are mostly volunteers. High-profile elections, particularly in presidential election cycles, may heighten risks to infrastructure.

Foreign attempts to interfere in recent U.S. elections have made for major news headlines. The dynamic between the elections process and related institutions—mainstream and social media, political campaigns, and political parties—is interconnected, but imprecise. Measuring election security efforts using voter turnout or public confidence levels as barometers of success can be equally challenging. However, proactively releasing accurate information and monitoring election-related news stories for accuracy are extremely important.

Figure 2. Election Infrastructure Subsector Snapshot
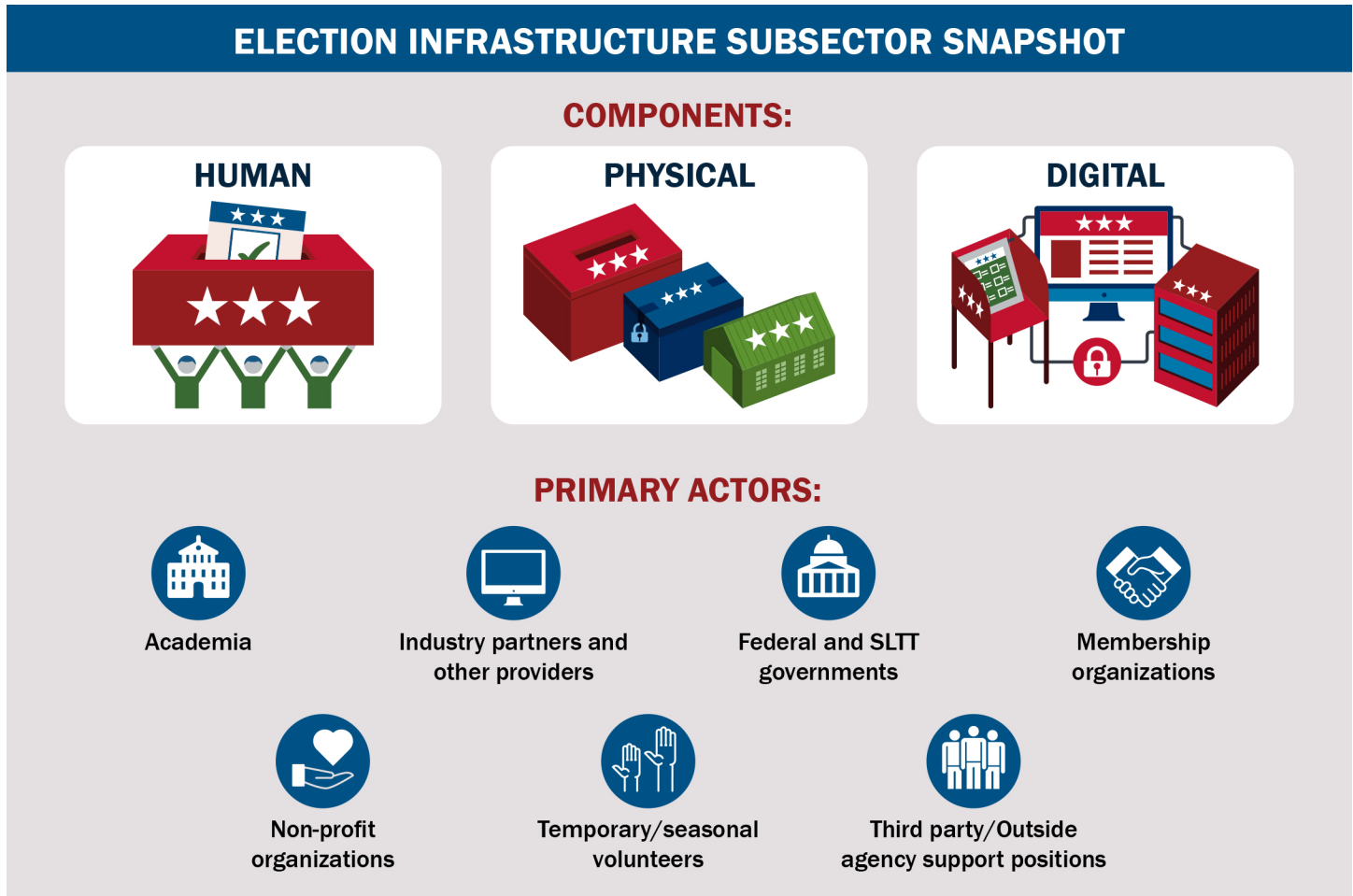
1.1.2 Components, Systems, and Networks

As identified by DHS in its designation, the Election Infrastructure Subsector encompasses physical, technological, and human elements necessary to conduct elections. The following is a list of Subsector components and assets:

KEY PHYSICAL COMPONENTS: Equipment and materials, facilities, and records that support or provide protection for the Subsector.

- **Voting Locations** – Facilities used by election officials to enable voters to cast ballots in person, which constitutes a significant proportion of total votes. Continuity of the voting process is dependent on the availability of voting locations and their ability to provide security and any other systems required to operate the voting process.
- **Technical Facilities** – Facilities used to house servers and network equipment, which can be a mix of onsite, offsite, or co-located facilities. Also, there may be separate facilities used to generate ballot files and tabulate votes.
- **Storage Facilities** – Includes warehouses or other similar facilities used to house equipment when not in use.

EXHIBIT 2

- **Processing Facilities** – Facilities used to print ballots, sample ballots, or polling place supplies. These facilities are either onsite or at a contractor's facility and must have adequate security and protection from the elements to ensure voting processes continue.

- **Administrative Facilities** – State, local and tribal election offices where election officials carry out their election administration duties.

- **Voting Hardware** – Ballots, poll books, machines, and records, as well as the physical equipment that supports digital systems that must be stored securely and protected.

KEY TECHNOLOGICAL COMPONENTS: Hardware and software components critical to supporting the election security mission, including computers, servers, databases, and other IT systems and assets used in Subsector activities to fulfill one of the following functions:

- **State and Local Networks** – Systems to conduct daily government functions, which may indirectly impact or connect with election system components, including email networks and other state and local-level systems, such as the Department of Motor Vehicles (DMV) systems.

- **Voter Registration Systems** – Systems used to collect personal voter information, including residency address, age, and other information required to determine voter eligibility and prevent duplicate voting. These systems are maintained at the local jurisdiction, the state level, or a combination of both. Administrative access varies by state and can include security protocols like multifactor authentication.

- **Election Systems** – Systems used to manage the entire voting process, which can include addresses, precincts, political and taxing districts, contest parameters, poll workers, voters, candidates, ballot layout, and the casting of votes.

- **Election Management Systems** – Sets of processing functions and voting system databases that define, develop, and maintain election databases; perform election definitions and setup functions; format ballots; and maintain audit trails.

- **Tabulation Systems** – Systems used to record votes, then accumulate and present them. Votes may be recorded on paper, directly onto voting machines, or both, including through Direct Recording Electronic (DRE) machines, or optical scanners used to cast paper ballots marked by hand or with a Touch Screen Ballot Marking Device (BMD).

- **Results Reporting** – Election-night reporting systems that generate and display unofficial results. These systems can be online systems, locally hosted systems, or a combination of both. These systems operate by uploading count data to the application, which then displays those totals in relationship to the overall population of a given jurisdiction.

- **Public Information Systems** – Systems that provide the public with general information about the election process, upcoming elections, and election results. These systems can also offer individual-level information regarding registration status, provisional ballot status, mail ballot status, or voting location, or support blank ballot delivery.

- **Electronic Poll Books** – Systems used by workers at polling places or voting centers to determine the eligibility of voters and the voters' correct ballot style. Some electronic poll books allow jurisdictions to update voter records or register voters for the first time. Electronic poll books used to update voters' addresses or register new voters typically will be connected to the internet.

- **Internal Production Software and Servers** – Various software platforms and servers that support the election infrastructure environment. This includes but is not limited to geographic information systems (GIS), which support the creation and assignment of eligible voters into various political and election-specific subdivisions.

KEY HUMAN COMPONENTS: Personnel with specialized training, certification, knowledge, skills, authorities, or roles whose absence could cause undesirable consequences or hamper the election security mission.

- **Strategic and Operational Positions** – Elected and appointed officials at the state and local level, such as local election officials, state election directors, State Chief Election Officials, industry and non-profit executives, and others who make up the leadership of the Subsector. These individuals operate election systems and have an in-depth understanding of their functionality. Their subject matter expertise ensures the operability of the election system. This includes operators of voting systems and related technology.

- **Temporary/Seasonal Support Positions** – Individuals selected on a short-term basis to carry out specific tasks essential to the conduct of elections, including temporary office staff, poll workers, and individuals outside the direct supervision of election officials.

EXHIBIT 2

1.2 Subsector Partners

The Federal Government, as well as state, local, tribal, and territorial (SLTT) governments; membership organizations and associations; election technology providers and other commercial entities; non-profit organizations; and academia must actively engage as a community to ensure the security and resilience of the Subsector.

A variety of private sector stakeholders are involved in election-related activities. Media organizations inform the public of election-related news and preliminary election results. Nonpartisan, non-profit organizations fill numerous roles, including compiling security best practices and facilitating state cooperation, voter outreach, and civic engagement.

Figure 3. Election Infrastructure Subsector Partnership Structure
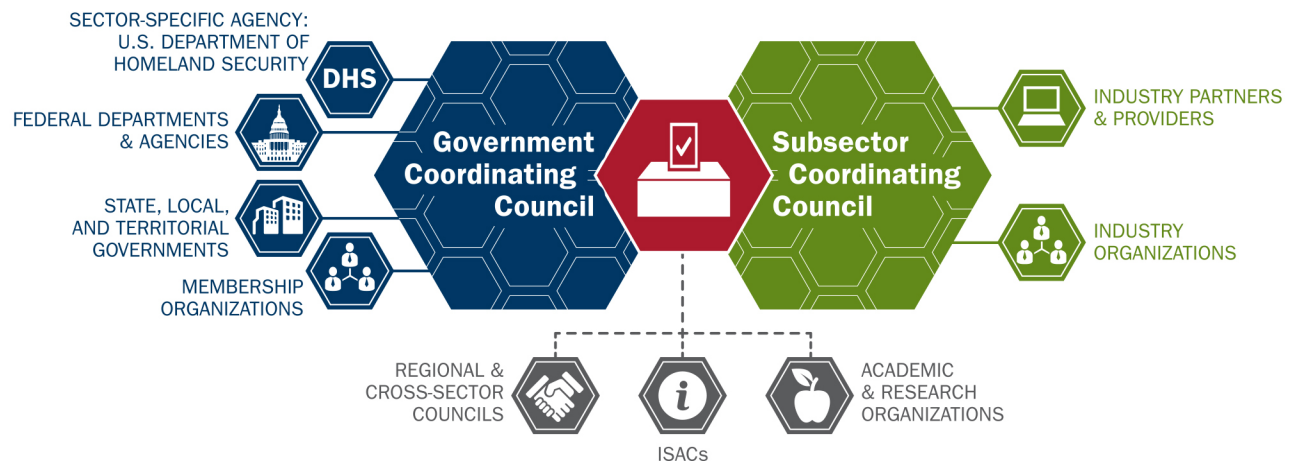
1.2.1 Coordinating Councils

The Election Infrastructure Subsector has diverse operations that are interdependent and interconnected with those of other infrastructure sectors. Individual Subsector entities proactively manage risk to their own operations and those of their customers through monitoring and mitigation activities. The decentralized nature of the Subsector offers a certain level of inherent resilience, with incidents in one jurisdiction not necessarily affecting neighboring jurisdictions. However, that structure also presents challenges and opportunities for coordinating public and private sector preparedness activities. The GCC and SCC were formed to help bridge this gap and to engage the owners, operators, and providers of election infrastructure assets in Subsector activities.[6]

Figure 4. Critical Subsector Dependencies

---
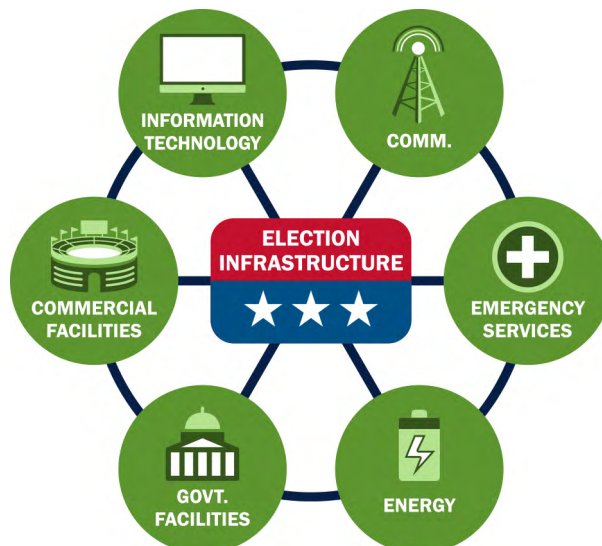
[6] GCC established October 2017. SCC established in February 2018.

EXHIBIT 2

Election Infrastructure Subsector Government Coordinating Council

The Election Infrastructure Subsector GCC is a government partnership council with the primary goal of sharing election security information among governments at the federal, state, and local levels and collaborating on best practices to mitigate and counter threats to election infrastructure. Members include the federal, state and local government agencies that own, operate, or administer physical or digital/cyber assets, systems, and processes related to the conduct of elections or that have responsibility for supporting the security and resilience of those assets, systems, and processes. The GCC consists of 24 state and local government representatives, including Secretaries of State, state election directors, and county/local election administrators. The GCC also has three Federal Government representatives: one from DHS and both the Chair and Vice Chair of the U.S. Election Assistance Commission (EAC). The National Institute of Standards and Technology (NIST), the Department of Defense's Federal Voting Assistance Program (FVAP), the Federal Bureau of Investigation (FBI), and representatives from other divisions of DHS are non-voting, ex officio members of the GCC. The GCC, governed by an operating charter, held its first meeting on October 14, 2017, and convenes in person at least twice a year.

Election Infrastructure Subsector GCC Executive Committee

The Election Infrastructure GCC formed an executive committee composed of a representative from each of the five stakeholder groups that make up the GCC to drive action on priorities between meetings. Those members are: the Director of the DHS National Risk Management Center (NRMC), the Chair of the EAC, the President of NASS, the President of the National Association of State Election Directors (NASED), and a local election official chosen from among Election Center and International Association of Government Officials (iGO) by the local election officials on the GCC.

Election Infrastructure Subsector Coordinating Council

The SCC for private sector election infrastructure providers was established in February 2018 with the adoption of its operating charter. The Council provides election industry stakeholders whose services, systems, products, or technology are used by (or on behalf of) state or local governments in administering the U.S. election process with a self-governing forum for voluntary interaction between themselves and with their GCC counterparts, as outlined in PPD-21. The SCC had 29 members organizations as of November 2019, representing the diverse spectrum of state and local election partners involved in supporting Subsector operations, including one ex-officio member: the IT-ISAC's EI-SIG. Members represent the Subsector in discussions with other critical infrastructure sectors as well. The Council meets in person at least twice annually.

Election Infrastructure SCC Executive Committee

The Election Infrastructure SCC maintains a five-member executive committee to guide the work of the Council and to coordinate with leadership counterparts from the GCC, the Cross-Sector Coordinating Council, and other individual sector councils. Members of the SCC include an elected Chair, a Vice Chair, the Past Chair and two Members-at-Large.

Working Groups

The GCC and SCC leverage working groups of Subsector representatives to pursue specific initiatives. Through the Critical Infrastructure Partnership Advisory Council (CIPAC), the Councils form joint council working groups made up of GCC and SCC members and subject matter experts. New working groups may be established at the direction of the Executive Committees as needed to take on specific tasks. The GCC and SCC use this working group structure to pursue the goals and objectives outlined in this SSP.

Subsector Partners

The SCC and GCC are organized to ensure that critical functions and responsibilities in government and the private sector are represented in the partnership.

1.2.2 Federal Agency Leadership

Sector-Specific Agency

DHS is the designated Subsector-Specific Agency (SSA) for the Election Infrastructure Subsector. DHS coordinates partnership activities and information sharing and is the primary federal interface with Subsector stakeholders for security and resilience. The Cybersecurity and Infrastructure Security Agency (CISA) fulfills the role of SSA for DHS through the NRMC, with the Assistant Director for the NRMC as a member of the Election Infrastructure Subsector GCC Executive Committee.

EXHIBIT 2

The U.S. Election Assistance Commission

The EAC is an independent, bipartisan federal agency charged with developing guidance to meet requirements set forth under HAVA, developing and adopting voluntary voting system guidelines, and serving as a national clearinghouse of information on election administration. The EAC also accredits testing laboratories, certifies voting systems, disburses HAVA funding when available, and audits state use of HAVA funds.

1.2.3 Cross-Sector and Regional Efforts

Members of the Subsector interact with other critical infrastructure sectors through participation in the cross-sector working groups, membership in other sector councils, and periodic discussions with representatives from other sectors. For example, in November 2018, the Election Infrastructure SCC selected a representative to serve on the Critical Infrastructure Cross-Sector Council's Black Sky Hazards Coordination Working Group, which is a joint effort to educate all sectors about the causes and effects of long-term power outages and the importance of developing cross-sector recommendations.

Additionally, DHS and a number of states have initiated regional initiatives for collaboration on preparedness and response activities. Fusion centers, the U.S. National Guard, and Federal Emergency Management Agency (FEMA) coordinators may also be involved in a state or local jurisdiction's cyber or physical security response planning to ensure strong coordination.

The U.S. Postal Service (USPS) is another critical government partner in election administration. Along with handling an increase in voting by mail throughout the country, the USPS plays an essential role in handling ballots for overseas citizens and active duty military voters. Election officials interact with local and regional postal officials to ensure the timely and secure delivery of mail ballots and related voter materials going to and from their offices. USPS National Change of Address (NCOA) Program data is also used to verify the accuracy of state voter registration lists.

1.3 Value Proposition for Participation in Subsector Partnership

Partnerships can provide participants mutual access to subject matter experts, training programs, educational opportunities, and information-sharing mechanisms. As the Subsector redoubles efforts to address challenges posed by diverse technologies, evolving threats, and a spectrum of risk across jurisdictions, the Election Infrastructure Subsector partnership structure provides:

- trusted mechanisms for information exchange with the Federal Government and Subsector stakeholders, including for the development, validation, and sharing of best practices;
- improved access to actionable, timely, and accurate threat information;
- access to and influence in the development of exercises, training, tools, and resources to meet evolving operating conditions; and
- inclusive processes for understanding and addressing vulnerabilities.

Participating in the public-private partnership improves SCC members' situational awareness and understanding of Subsector risks, enabling members to more effectively:

- minimize disruptions and improve resilience to ensure free, fair, and secure elections; and
- raise awareness of actions taken in support of preparedness, continuity, and the proactive management of election system risks to maintain and enhance public confidence in election systems.

The Subsector partnership can also be used to address those needs for which no viable private sector solution exists, or to identify high transaction costs or legal barriers that could cause significant coordination or implementation challenges for potential solutions.

EXHIBIT 2

2. RISK MANAGEMENT: ASSESSING AND MITIGATING RISK

The NIPP 2013 Risk Management Framework[7] provides a common approach for election infrastructure stakeholders to identify their infrastructure, assess and analyze their risks, and identify and prioritize risk management activities. The goals and objectives discussed in this SSP are rooted in this Framework.

Identifying Infrastructure

Election infrastructure exists at the federal, state, and local levels; is owned/operated by the government and the private sector; and includes a range of physical and IT assets, networks, and systems. Specific infrastructure may be unique to a given jurisdiction, but there are commonalities across all jurisdictions. A detailed description of the components that must be considered as part of any thorough risk analysis and management process is discussed in *Section 1.1.2*.

Assess and Analyze Risks

Risk assessments examine vulnerabilities, threats, and consequences to ascertain and analyze risks to help election infrastructure stakeholders prioritize management strategies. Individual Subsector members—governments and private sector partners—perform risk assessments for their critical assets.

Completed risk assessments should be documentable, reproducible, and defensible. To support individual stakeholders' efforts to effectively analyze risks and identify interdependencies, Subsector partners employ a variety of mechanisms that include:

- publication of an overall Election Infrastructure Risk Characterization
- classified threat briefings from federal agencies for Subsector members with security clearance, as well as unclassified briefings from private sector firms
- information sharing through established forums, such as Fusion Centers, the Homeland Security Information Network – Election Infrastructure Subsector (HSIN-EIS), the EI-ISAC, the EI-SIG (for private sector providers), conferences, and organizational trainings and exercises
- tabletop exercises hosted by Subsector partners that identify gaps in security, procedures, and communication protocols
- DHS offerings, including vulnerability assessments, cyber assessments, evaluations, informational products, and reviews

Implementing Risk Management Activities

The Subsector has numerous, diverse risk environments, requiring election infrastructure stakeholders to prioritize their risk management activities to address their specific needs. In addition to individual risk management activities, the Subsector actively participates in risk management activities that include:

- tabletop exercises that include federal partners to test Subsector and individual member plans
- topic-specific workgroups to exchange information, discuss needs, and develop plans to address identified needs
- election security training and exercises for partners across the Subsector, tailored to fit the needs of the individual partner (whether SLTT government or private sector)
- organizational trainings, exercises, and assessments, such as counter-phishing campaigns and cyber hygiene reviews
- promotion of risk-informed security controls and processes, such as risk-limiting audits

Concern for an appropriate degree of public disclosure around election threats and vulnerabilities plays a significant role in determining what information about individual vulnerability assessments partners may share. These voluntary assessments are carefully guarded because they identify specific vulnerabilities in a physical site, a system/process point, or a company/organization. However, Subsector industry providers frequently work with federal, state, and local government agencies to leverage partner resources in conducting risk assessments that contribute to regional or national security and resilience,

---

[7] Under the NIPP 2013 Risk Management Framework, risk is the potential for an adverse outcome from an event, determined by the event's likelihood—a function of the specific threats and vulnerabilities—and associated consequences if the event occurs.

EXHIBIT 2

as demonstrated by current SSA initiatives. Time constraints, concerns about exposing vulnerabilities or proprietary information, and assessment-related expenses are factors that may limit the ability of some Subsector partners to participate or share information more broadly.

Risk assessment and mitigation is an ongoing process that requires partners to maintain a high level of threat awareness, as well as the capacity to respond to an increasing number of complex challenges. By applying the NIPP 2013 Risk Management Framework, the Subsector will continually evaluate the threat landscape and adapt as necessary to meet emerging threats and challenges.[8]

A number of resources are also available from the Federal Government that can support Subsector partners. For example, CISA has provided regional coordination and field operations support, including Protective Security Advisors (PSA) and Cybersecurity Advisors to assist owners and operators with voluntary risk assessments. DHS also operates several voluntary programs to allow owners and operators to report vulnerabilities in election technology. The EAC also has a mandatory reporting requirement in place for voting systems manufacturers, which increases visibility of known vulnerabilities for potentially affected users so they can be addressed.[9]

---

[8] National Infrastructure Protection Plan's Risk Management Framework, 2013, https://www.dhs.gov/xlibrary/assets/NIPP_RiskMgmt.pdf.

[9] EAC Voting System Testing and Certification Program Manual: 2.3.2.7. *Report to the Program Director any known malfunction of a voting system holding an EAC Certification*, June 1, 2011.

EXHIBIT 2

FUNDING

It is impossible to make an honest assessment of the Election Infrastructure Subsector's risk and the potential to mitigate that risk without an understanding of the chronic resource issues the Subsector faces at all levels of government. While much of this plan focuses on what can be done to assess and mitigate risk, a certain amount of what can be done is dependent on sufficient funding. If election officials are unable to replace antiquated or unsupported systems in a timely fashion, additional vulnerabilities and risk to the system are created. If election administrators are unable to hire sufficient technical support staff or provide sufficient training to existing staff, this too has real consequences.

The designation of elections as critical infrastructure in 2017 brought resourcing issues to the forefront, particularly at the federal level. In March 2018, Congress appropriated the remaining $380 million in federal funding from HAVA, and the EAC disbursed all funds to the states by August 2018. In December 2019, Congress added another $425 million in one-time funding under HAVA. To complement this effort, the GCC released a procurement guide to help election officials take cybersecurity into account as they spend those funds, as well as potential future funds.

There is widespread agreement among election officials that more resources—and, importantly, more sustained resources—are needed. That theme is shared across the critical infrastructure sectors: one of the key findings of the Nationwide Cybersecurity Review was that SLTT communities consistently rank a lack of sufficient funding as a top-5 security concern.[10] Funding shortages impact both state and local election officials, though in different ways. The one-time disbursement of the remaining HAVA funds forced some states to choose between conducting necessary state-level improvements and providing local election officials with meaningful funds. For example, some states needed to replace, upgrade or harden their statewide voter registration database. In most states, the statewide voter registration database is used at all local election offices and must be protected for election administration purposes, but also to protect voters' personally identifiable information. In other states, it was crucial to replace aging voting equipment at the municipal or county level. These examples show that state and local priorities must both be addressed, and future funding increases are necessary to ensure that state and local election offices do not need to compete for the same limited funding, but have the resources needed to fully protect our democracy.

While such federal infusions are important and welcome, for the Election Infrastructure Subsector to succeed, a government-wide approach to funding elections and election security is needed. Viewing the Subsector as an "infrastructure" of our democracy is important to understanding the need for consistent investment and maintenance to ensure the system is strong. SLTT governments are primarily responsible for the administration of elections and should also be primarily responsible for funding elections. This requires tough choices at the state and local levels, where election funding has too often been neglected. However, the critical infrastructure designation came about because of unprecedented threats by hostile nation-state actors. This new dynamic requires federal investment to assist SLTT governments as well. Such investments will never and should never replace the SLTT role in funding election administration but are needed to increase defensive capacity and coordination amongst SLTT governments and their federal partners to secure the Election Infrastructure Subsector.

Legislative interest in election security has also greatly increased since 2017, both at the state and federal levels. In 2019 alone, Congress held more than a dozen hearings about election security and have testified to the progress made by the sector since 2016. Subsector partners have spent hours educating Members of Congress and state policymakers, as well as the public, about how elections work and the work happening in the Subsector. Election infrastructure partners are committed to ensuring that stakeholders have a clear understanding of election administration and systems, including how they are developed, certified, tested, and secured.

---

[10] Center for Internet Security (CIS), Nationwide Cybersecurity Review: Summary Report, 2017, https://www.cisecurity.org/wp-content/uploads/2018/10/NCSR-2017-Final.pdf.

EXHIBIT 2

3. VISION, MISSION, GOALS, AND OBJECTIVES

This chapter outlines the goals and objectives that will guide Subsector partners' ongoing efforts to enhance the security and resilience of the elections they conduct and support. The associated activities are designed to provide direct and indirect support to election administrators, improve awareness of election security efforts and needs within the Subsector and among the public, and ultimately promote the sustained investment necessary to ensure continued public confidence in the results of U.S. elections.

3.1 Subsector Vision and Mission

ELECTION INFRASTRUCTURE SUBSECTOR VISION

"A unified government and private sector approach to empower the election stakeholder community to build resilience to election infrastructure risks."

ELECTION INFRASTRUCTURE SUBSECTOR MISSION

"To coordinate efforts by state and local election officials, private sector and non-profit partners, and the Federal Government to manage risks and secure election infrastructure against new and evolving threats."

PUBLIC CONFIDENCE IN ELECTION OUTCOMES

Research into what shapes and affects voter confidence in election results has repeatedly shown that most Americans are generally confident that the election process counts votes accurately and the administration of elections in their communities is well-managed. In 2018, the Pew Research Center found that about eight in ten American voters went into that year's General Election believing it was very or somewhat likely that votes would be counted as intended.[11] However, social influence and misinformation campaigns seek to erode that confidence by targeting the social underpinnings of our democracy. Though any causal link between voter confidence and turnout is tenuous at best,[12] the members of the Election Infrastructure Subsector believe strongly that all American voters should be assured that their votes will count as cast, and all eligible voters should be able to freely exercise their right to vote without serious disruption or interference.

The Subsector was formed to bolster this confidence and improve our national security posture through the implementation of security best practices, as well as to improve information sharing between American voters and the officials, agencies, and private industry partners and other organizations responsible for overseeing elections.

Research conducted by scholars who focus on voters' experiences when casting a ballot shows that Americans feel more confident that their vote will be counted accurately when the voting process is quick and the election officials/poll workers are professional and knowledgeable.[13] And so the Subsector seeks to speak with a unified and direct message to the American public: every voter deserves a voting experience that is easy to navigate, is transparent, and leaves a secure sense that every vote will be tallied accurately.

3.2 Joint Goals and Objectives

This section outlines the goals and objectives for how best to support the Subsector's continuing effort to secure the essential belief that Americans have confidence in their elections. This is done by increasing awareness internally and externally, providing direct support to administrators, and securing the necessary short-, medium-, and long-term investments. The goals provide a framework to guide resilience efforts and improve Election Infrastructure Subsector risk management practices.

---

[11] The Pew Research Center, "Elections in America: Concerns Over Security, Divisions Over Expanding Access to Voting," October 29, 2018, https://www.people-press.org/2018/10/29/elections-in-america-concerns-over-security-divisions-over-expanding-access-to-voting/.

[12] MIT Election Data + Science Lab, "Voter Confidence," 2019. https://electionlab.mit.edu/research/voter-confidence.

[13] Ibid.

EXHIBIT 2

Table 1. Election Infrastructure Subsector GCC and SCC Joint Goals and Objectives

JOINT NATIONAL GOALS	JOINT OBJECTIVES
COMMUNICATION	**Expand availability and increase awareness of threat information and efforts to secure U.S. elections among Subsector partners and the public.** **a. INFORMATION SHARING:** Foster a voluntary, multi-directional information-sharing environment which ensures Subsector partners understand threats, risks, and vulnerabilities they face and understand their options for reporting detected or suspected threats or incidents. **b. INCLUSION:** Expand the reach of Subsector communication to include more local election jurisdictions and smaller industry providers, as well as other critical infrastructure sectors, to improve coordination and understand critical dependencies. **c. AWARENESS:** Play an active role in informing policy makers to help them and the public understand issues around election security to enable the flow of accurate, timely, and relevant information.
CAPACITY	**Support risk assessment and management, emergency planning, and incident response.** **a. READINESS:** Create a continuous training and learning environment for election officials and industry partners to build knowledge and skills around cyber hygiene, risk assessments, and critical infrastructure security and resilience activities. **b. RESPONSE:** Provide subject matter expertise to support the creation and routine exercise of election-related incident response plans. **c. MITIGATION & PROTECTION:** Strengthen awareness and management of threats to election infrastructure that may result in significant disruption or harm to the conduct of elections, including physical and cybersecurity threats as well as risks associated with dependencies and interdependencies.
RESOURCES	**Assist Subsector partners in determining priorities, programs, and budgets for securing their entities and assets.** **a. INVESTMENT:** Develop consistent and sustainable sources of support from local, state, and federal levels as well as non-profits and the private sector for election security measures that are appropriately flexible and based on the threat landscape. **b. RESEARCH:** Identify resource and knowledge gaps in securing election infrastructure to build tools and programs for Subsector-wide use.

3.3 Joint Subsector Activities

This section outlines and describes activities the Subsector has completed, is working on, or plans to complete to meet the goals and objectives above. The activities below are broken up into Communication, Capacity, and Resources to align with the goals. The tables below assign each activity to the appropriate council(s) and provide a status update on how Subsector activities are progressing as the Subsector partnership continues to mature.

The Subsector continues to explore how to best quantify voluntary partnership activities' contribution to risk reduction and enhanced resilience across the election infrastructure landscape. Efforts to assess Subsector efforts are an assessment of our accomplishments as a Subsector and a recognition of future Subsector needs and are not a statement about the efforts of any individual Subsector partner.

EXHIBIT 2

3.3.1 Communication

Expand availability and increase awareness of threat information and efforts to secure U.S. elections among Subsector partners and the public.

a. **INFORMATION SHARING** - Foster a voluntary, multi-directional information-sharing environment which ensures Subsector partners understand threats, risks, and vulnerabilities they face and their options for reporting detected or suspected threats or incidents.

b. **INCLUSION** - Expand the reach of Subsector communication to include more local election jurisdictions and smaller industry providers, as well as other critical infrastructure sectors, to improve coordination and understand critical dependencies.

c. **AWARENESS** - Play an active role in informing policy makers to help them and the public understand issues around election security to enable the flow of accurate, timely, and relevant information.

ELECTION SUBSECTOR ACTIVITY	STATUS	COUNCIL
Finalize, adopt, and distribute Version 1.0 of the Communications Protocols for voluntary two-way sharing	**GCC – Complete**, July 2018 **SCC – Complete**, October 2018	GCC and SCC
Apply lessons learned to improve Subsector-wide communications	**In Progress** – Communications Working Group assigned to update to Communication Protocol Version 2.0. SCC updated Incident Response & Reporting Guidance in September 2019	GCC and SCC
Design and adopt Digital Network to facilitate communication across the Subsector	**In Progress** – Joint Digital Network Development Working Group assigned to assess needs and make recommendations	GCC and SCC
Develop and refine an outward-facing strategic communications plan for coordinated messaging	**In Progress** – Communications Working Group assigned to develop a national emergency response communications plan	GCC
Provide members of the Subsector with the knowledge and tools necessarily to educate stakeholders and the public about election security	**Ongoing** – NASS, NASED, Election Center, iGO, and state conferences and distribution lists regularly provide Subsector members with details about tools and trends they can use to educate themselves and their voters	GCC and SCC
Establish Information Sharing and Analysis Centers for the Subsector that provide options for governments and private sector partners	**Complete** – The EI-ISAC established in February 2018 (GCC) and the EI-SIG established within the IT-ISAC in August 2018 (SCC)	GCC and SCC
Increase membership in the EI-ISAC for state and local election offices and private sector partners, as well as the EI-SIG for private sector partners	All 50 states and five territories belong to the EI-ISAC, which has more than 2,300 members as of January 2020. The EI-SIG established in 2018	GCC and SCC
Increase enrollment in the Subsector Clearance Program in order to increase understanding of risks and threats among Subsector partners	**Ongoing** – Phase 3 and expanded private sector nominations began in 2019 to increase SLTT and private sector representatives with clearance. As of January 2020, 162 individuals have received clearance	GCC and SCC
Promote membership growth in the SCC in order to ensure Subsector coverage	**Ongoing** – As of November 2019, the SCC has 29 members	SCC

EXHIBIT 2

ELECTION SUBSECTOR ACTIVITY	STATUS	COUNCIL
Inform policy makers on Subsector efforts around election security	**Ongoing** – GCC and SCC members regularly testify to Congress and inform state and local policy makers. Jointly, the GCC and SCC issued a statement on the Senate Intelligence Committee Report Volume[14]	**GCC** and **SCC**
Coordinate with other critical infrastructure sectors to increase readiness for large-scale cross-sector emergencies	**In Progress** – SCC members engage with the Cross-Sector Coordinating Council, including the Black Sky Hazards Coordination Working Group	**SCC**

Improving communication across the Subsector is central to the work of both the GCC and SCC. Subsector partners learned from past communication failures and have made substantial progress in information sharing among partners as well as with policy makers and the public. These efforts continue as described below.

Information Sharing

Information sharing is a critical tenet of the Subsector's objectives; the first substantive document approved by the GCC in 2018 was a set of Communications Protocols that guide how, when, and to whom incidents are reported by SLTT election officials. Currently, the GCC Communications Working Group is evaluating these protocols to apply lessons learned from 2018 to strengthen the document for 2020 and beyond. Meanwhile, the SCC updated its incident reporting and response guidance in September 2019.

The decentralized nature of the Subsector presents challenges related to information sharing: we must build mechanisms for sharing information between the Federal Government and SLTT partners; between states and their local election jurisdictions; and between federal/SLTT governments and private sector partners. Each level is as important as the next, and trust is paramount. Engagement across levels of government and across the Subsector have helped to build trust, and these efforts continue.

DHS uses the Homeland Security Information Network (HSIN) as a digital communications platform in most other critical infrastructure sectors, but the platform has thus far had less success in the Subsector due to challenges around awareness, usability, and accessibility of the platform. A joint Digital Network Development Working Group is reviewing current practices for digital information sharing and making recommendations for improvement. While the Digital Network remains under development, currently, information is typically shared from federal to state to local entities via more informal communication methods, and from local to state to federal using both formal and informal mechanisms. The Working Group is determining how to improve access to and participation in HSIN among election officials and small industry providers, all of whom have struggled with accessing and using the platform.

The establishment and growth of the EI-ISAC are significant components of the Subsector's information and threat intelligence sharing capability. Through the EI-ISAC, SLTT election offices and private sector and non-profit EI-ISAC members can exchange anonymized technical indicators and threat information with each other, federal partners, and the private sector, and the Federal Government is able to efficiently share similar information with SLTT election offices and election infrastructure providers. The EI-ISAC is a member of the National Council of ISACs (NCI), allowing them to take advantage of information from other ISACs, and is collocated with the Multi-State Information Sharing and Analysis Center (MS-ISAC), which serves SLTT governments in other sectors. Further, the MS-ISAC has a representative on the DHS National Cybersecurity and Communications Integration Center (NCCIC) floor, allowing for efficient exchange of information with the Federal Government. Any private sector partner with a contract with a state or local election office is eligible to be a Supporting Member of the EI-ISAC, allowing them to benefit from the information shared by EI-ISAC members.

Additionally, in August 2018, the IT-ISAC approved the formation of an EI-SIG to provide a dedicated and trusted forum within the IT-ISAC for election industry stakeholders to help guard their networks and assets against physical and cyber threats. The goal of the EI-SIG is to scale up the sharing that occurs between election industry providers and other IT companies to help understand the broader threats to election technology and systems. The EI-SIG also helps members build capacity by providing additional services and learning opportunities that are not available to companies as supporting members via the EI-ISAC.

---

[14] U.S. Senate, *Select Committee on Intelligence: United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*, 2019, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

EXHIBIT 2

The Election Infrastructure Subsector Clearance Program is another component of information sharing within the Subsector. DHS sponsors security clearances for Subsector stakeholders. The government clearance program started before the private sector clearance program, but both programs continue to grow.

ELECTION INFRASTRUCTURE SUBSECTOR CLEARANCE PROGRAM

State Chief Election Officials are eligible for secret-level security clearance and can designate additional members of their staff to receive clearance. Nominated local election officials can also receive clearance. This program deployed in phases, starting in 2017:

- **Phase 1 (2017):** State Chief Election Officials and all GCC members
- **Phase 2 (late 2017):** Two additional state-level officials
- **Phase 3 (early 2019):** Up to three additional nominees per state, including one nomination from the State Chief Election Official, one nomination from the head of the state's local election officials' or clerks' association (or other appropriate organization), and one nomination from CISA regional staff.

Uniquely, the Election Infrastructure Subsector experiences regular turnover as a result of elections. New State Chief Election Officials and state-level staff frequently need to be brought into the clearance program. Each State Chief Election Official is able to nominate the staff of their choosing as part of the Phase 2 program, even if there are others in the office who received clearance under the previous State Chief Election Official. Finally, State Chief Election Officials can designate someone else in their office to receive the Phase 1 clearance in their place. State Chief Election Official (Phase 1) clearance has no bearing on the Phase 2 clearances.

Beginning with the creation of the Election Infrastructure SCC, all SCC primary representatives and alternates are eligible for secret-level security clearance. In 2019, the program expanded to include an additional three private sector partners per state or territory, regardless of their relationship to the SCC. The additional three can be nominated by the State Chief Election Official or a DHS representative.

The SCC also coordinates with other critical infrastructure sectors via the Critical Infrastructure Cross-Sector Council to increase readiness for large-scale incidents and emergencies of national or regional significance. The Cross-Sector Council facilitates consultations, information sharing, and coordinated effort across the critical infrastructure sectors and subsectors and with the Federal Government, as well as with the SLTT Government Coordinating Council (SLTT GCC), the Regional Consortium Coordinating Council (RC3), and the NCI.

The Election Infrastructure SCC participates in the Black Sky Hazards Coordination Working Group, which aims to assure awareness and inform preparedness efforts for extended power outages from natural or intentional causes, including an electro-magnetic pulse (EMP) situation that could shut down electricity in an affected area for an extended period of time. Participants representing each sector can contribute and receive valuable preparedness information for sharing with organizations across their respective industries.

Inclusion

Now that the GCC and SCC have moved beyond establishment, and as Subsector processes mature, Subsector partners are committed to increasing participation in activities among local election officials from small-to-medium jurisdictions, as well as smaller industry providers.

Increasing local membership in the EI-ISAC has been, and continues to be, an important focus for GCC members. DHS representatives, EI-ISAC staff, and state election officials regularly attend local election official conferences and work directly with local election officials to encourage participation in the EI-ISAC. In 2019, the EI-ISAC established an Executive Board composed of a diverse mix of state and local election officials and IT staff. The establishment and launch of the EI-ISAC is one of the most important early accomplishments for the Subsector, and it has greatly improved access to threat information for election officials and industry providers. The Subsector has realized 100 percent participation in the EI-ISAC from state election offices, four of the five U.S. Territories, and the District of Columbia.

EXHIBIT 2

However, while local EI-ISAC membership has grown significantly (as of the end of 2019, more than 2,300 local election jurisdictions had joined), more work can be done to extend membership to mid-size and smaller jurisdictions. The initial mission of the EI-ISAC Executive Board is to develop strategies for including more local election jurisdictions. While the Election Infrastructure Subsector takes pride in having the fastest-growing ISAC ever, it is clear that communications and services from the EI-ISAC need to continue to adapt to serve many local election jurisdictions better in order to ensure complete nationwide coverage.

Similarly, the major election industry providers are part of the SCC, but many smaller providers with business or operating interests in U.S. election infrastructure systems or services have yet to actively engage. The SCC has worked with their GCC counterparts to promote the benefits of SCC membership to these stakeholders, and several newer industry providers have also joined. All members of the SCC have the opportunity to join either the EI-ISAC or the EI-SIG, or in many cases, both. A list of EI-ISAC members is available at https://www.cisecurity.org/ei-isac/partners-ei-isac/.

Awareness

Election infrastructure has generated unprecedented public interest since its establishment as critical infrastructure in 2017. Educating members of the press and the public to better understand the progress made since 2016 remains an ongoing challenge. There is widespread concern that misleading or factually erroneous coverage focusing on vulnerabilities and failures in election systems can undermine voter confidence in the election process and result in long-term, downstream effects on voting. All members of the Subsector take seriously their responsibilities to ensure the security and integrity of elections, but progress can be difficult to measure and monitor.

Subsector partners regularly speak at in-state and national events and to the press, as well as testify before state legislatures and the U.S. Congress to demonstrate improvements and help educate and inform the public and other relevant stakeholders. They have made a concerted effort to empower members of the Subsector with the knowledge and tools necessarily to educate stakeholders and the public about election security.

Recognizing the importance of getting timely and accurate information to the public in the event of a widespread national incident, the GCC Communications Working Group is developing a proposed protocol for coordinated messaging across states and local election jurisdictions. The decentralized nature of elections, as well as the clear role of SLTT governments in running elections, makes this a challenge, as there is no natural spokesperson for the Subsector as a whole. Further, while states have NASS and NASED to communicate important election security information quickly and to the correct people, local election officials are much more difficult to reach during a crisis, both because they are greater in number and diversity, and, critically, because they are often in the field and away from their desks administering elections during high-stress periods.

The GCC and SCC also periodically make statements, both jointly and individually, to inform the public of efforts to secure elections. For example, they issued a joint statement on the Senate Intelligence Committee Report Volume 1 in 2019 that outlined efforts of the Subsector to protect elections from the threats outlined in the report.

3.3.2 Capacity

Support risk assessment and management, emergency planning, and incident response.

a. **READINESS** - Create a continuous training and learning environment for election officials and industry partners to build knowledge and skills around cyber hygiene, risk assessments, and critical infrastructure security and resilience activities.

b. **RESPONSE** - Provide subject matter expertise to support the creation and routine exercise of election-related incident response plans.

c. **MITIGATION & PROTECTION** - Strengthen awareness and management of threats to election infrastructure that may result in significant disruption or harm to the conduct of elections, including physical and cybersecurity threats as well as risks associated with dependencies and interdependencies.

EXHIBIT 2

ELECTION SUBSECTOR ACTIVITY	STATUS	COUNCIL
Develop and deploy an online training environment for election officials	**Incomplete** – Assigned to GCC Training Working Group	GCC
Work with the EAC, nonprofits, and others to identify relevant training offerings and expand adoption throughout the Subsector	**Ongoing** – GCC and SCC members have identified some relevant training offerings and promoted them to the broader Subsector, such as the Center for Technology and Civic Life's (CTCL) cybersecurity training for election officials; working groups will be formed to coordinate across the Subsector in 2020	GCC and SCC
Promote Subsector priorities, incident reporting protocols, and security controls for Subsector stakeholders through DHS Last Mile products	**Ongoing** – Last Mile products have been, and continue to be, designed and distributed	GCC and SCC
Promote DHS cybersecurity services for broad Subsector use. Provide input to DHS to help evaluate whether technical service offerings are scalable and ensure they empower Subsector members to effectively manage risk	**Ongoing** – 50 states and four territories work with DHS in some way; the GCC continues to promote these services to state and local election officials and provide feedback to DHS. Additionally, numerous SCC companies have taken advantage of these services	GCC and SCC
Advance how election entities understand and organize their cyber risk management efforts through common tools, including developing an Election Infrastructure Subsector profile of the NIST cybersecurity framework	**In Progress** – Assigned to the NIST Cybersecurity Framework Working Group	GCC and SCC
Work with DHS, the Intelligence Community, and the private sector to better understand risk to the Subsector. Identify obstacles or impediments to effective election infrastructure security and resilience protection programs and develop actions to mitigate them	**Ongoing** – DHS works with other federal agencies, the GCC, the SCC, and other private sector partners to provide classified and unclassified threat briefings	GCC and SCC
Address common and known risks by promoting and supporting widespread deployment of audits; Domain Based Message Authentication, Reporting and Conformance (DMARC); the DotGov (.gov) domain, where applicable; Hypertext Transfer Protocol Secure (HTTPS); and Two-Factor Authentication (2FA) by Subsector entities	**Ongoing** – Distribution of DHS Slick Sheets as well as conference presentations and other tools and resources	GCC and SCC
Facilitate improvement in vulnerability disclosures, when appropriate, to help close the gap between identification and mitigation	**In Progress** – EI-SIG development and coordination of an industrywide coordinated vulnerability disclosure (CVD) in progress. GCC partners to discuss as part of 2020 priorities	GCC and SCC each addressing separately
Explore ways that procurement practices can elevate security design considerations	**Complete** – GCC Funding Considerations document released May 2018. GCC and SCC members provided input on the Center for Internet Security (CIS) Procurement Guide, released April 2019	GCC and SCC
Execute an annual national tabletop exercise (Tabletop the Vote) and support state-specific tabletop exercises. Clarify the roles and responsibilities of Subsector partners in any federal or state-coordinated response, recovery, and reconstitution effort involving incidents/attacks	**Ongoing** – GCC and SCC help to facilitate an annual Tabletop the Vote exercise each year, led by CISA. Subsector members provide operational support to state-level exercises	GCC and SCC
Develop incident response plan templates for Subsector-wide voluntary use	**In Progress** – DHS "Incident Handling Overview for Elections" released 2018. New template for SLTTs planned for early 2020.	GCC and SCC each addressing separately
Work with trusted advisors to enhance resilience of key physical offices, sites, and facilities, including election equipment storage locations.	**Ongoing/continuous** for Subsector partners	GCC and SCC

EXHIBIT 2

Readiness

The GCC and SCC are jointly focused on increasing the capacity among election officials and private sector providers to effectively assess and manage risk to improve their security posture. A vital element of the capacity-building goal for the Subsector is providing training and resources that can help individual election entities and private sector providers build their own cybersecurity capabilities. The volume of training offerings related to election security has increased substantially since 2016:

- Federal Virtual Training Environment (FedVTE) training is provided to state and local officials by DHS, in collaboration with the EI-ISAC.

- Nearly every state provides annual training to their local election officials, which has been adapted or expanded in recent years to include cyber training.

- SCC member companies and organizations conduct companywide cyber hygiene training, internal drills and other employee-focused efforts to enhance cyber awareness and safety.

- In partnership with the International Council of E-Commerce Consultants, also known as EC-Council, the IT-ISAC offers professional cybersecurity training to EI-SIG member companies.

- Non-profit organizations and universities, such as the CTCL and Harvard's Belfer Center, also provide resources and training.

Subsector partners are actively promoting these training options among the broader Subsector; however, due to the decentralized nature of election administration and the sheer number of election officials and providers, it remains a challenge to ensure that local election officials and smaller industry providers are engaged in training and have awareness of/ access to these resources.

To help address this challenge, the GCC established a Training Working Group. The group has identified relevant training offerings, including those mentioned above, and has been tasked with developing and deploying an online training environment for election officials.

Finally, to promote recommended security practices, Subsector partners are working with DHS to create and distribute products intended to reach the broadest possible range of stakeholders. These include Last Mile posters for state and local election officials, and the SCC Election Security Guide for private sector providers, both of which provide documentation of shared objectives, incident reporting procedures, and security controls for their respective stakeholder groups. The posters and other products offer visual reminders about cyber hygiene and other pre-election security practices while providing cues for voters who are interested in the steps that election officials take to ensure the integrity of the vote.

Response

The Subsector continues to focus on preparing state and local election officials, as well as industry providers, for incident response. Annually, the Subsector executes a national tabletop exercise called Tabletop the Vote, a virtual tabletop exercise with participants from across the Federal Government and state and local election offices from nearly every state and territory, as well as industry partners. Partners participate in the development and the execution of this exercise and provide input on how to improve it each year. Tabletop the Vote allows participants to exercise their incident response plans while working through scenarios that include physical and cybersecurity threats. Federal Government partners practice what they would be doing and how they would coordinate and share information during the scenarios, also learning how state and local election offices would respond in a given situation. Feedback on Tabletop the Vote is consistently positive, and the Subsector plans to continue the exercise for the foreseeable future, with a focus on incident response planning.

DHS has worked closely with state and local election partners to simulate election cybersecurity events. One identified gap in incident response preparedness is the lack of incident response plans in many election offices. While state election offices have incident response plans (most of which incorporate state partners, including the State Chief Information Officer [CIO] or National Guard), many local election offices do not yet have incident response plans or have identified that their plans need further development. In response, state election offices, NASS, and NASED have distributed incident response planning resources to local election officials, and DHS is developing an incident response plan template for local election offices, expected by January 2020. Separately, the SCC Incident Management and Emergency Response Working Group was established to facilitate organizational readiness and incident response planning for the private sector to ensure elections continuity and recovery in case of an event with national critical significance and multi-jurisdictional impacts. The Working Group has identified risks and threats in three categories: Cybersecurity, Domestic Terrorism, and Natural Disasters.

EXHIBIT 2

Subsector members also participate in and support state-level tabletop exercises. They can be massive endeavors, enabling in-person participation from state and local election officials. Some states have had more than 400 participants from local jurisdictions, state offices, and the Federal Government. Through these exercises, state election officials have helped facilitate the creation and exercise of incident response plans for local election officials that complement the state plan and have helped local election officials understand the complexity of the cyber threats we face. While many states have used the Belfer Center's tabletop exercise as a model, others are thinking creatively about how to adapt the templates for their own use, including expanding the subject matter beyond security.

Mitigation & Protection

Understanding election infrastructure risk environments is an important aspect of capacity building, as it is key to determining priorities and allocating resources. Subsector partners created a Joint Cybersecurity Framework Working Group to develop a Subsector-specific risk profile using the NIST Cybersecurity Framework to advance how election stakeholders understand and manage their cyber risk. The goal is to allow for more mature risk conversations within the Subsector by building a shared understanding of risk that is applicable across diverse U.S. election stakeholders.

A major need to building a broad understanding of risk to the Subsector is to improve access to timely and actionable intelligence. Although both the Election Infrastructure Subsector Clearance Program and the establishment of the EI-ISAC have helped, opportunities for improvement remain. The Councils are pushing for more rapid release of intelligence through classified briefings, as much specificity as possible to support security decision making, and sharing of related unclassified information to support broader action. To augment information received by the Intelligence Community, the Subsector works with DHS and private sector entities to receive unclassified briefings from private sector cybersecurity firms based on threat intelligence collected from their work in the field, both domestically and internationally.

Based on risk assessment efforts, the Subsector continues to develop its understanding of the need for services and resources within the Subsector. The availability and use of cybersecurity services from DHS, the EI-ISAC, other state agencies, and other providers by election officials, particularly state-level officials, has increased significantly since the declaration of elections as critical infrastructure. The Subsector continues to work with DHS to provide input on the effectiveness of technical services offerings and to promote DHS services to local-level stakeholders and smaller industry providers. Engaging with and providing services to the approximately 9,000 local election jurisdictions in the U.S. presents a range of scalability challenges, including the difficulty in reaching local officials to ensure they know what services are available, how to access them, and what to do with the results.

Though there is significant diversity in how elections are administered throughout the U.S., the Subsector partnership has recommended specific security measures that state and local election officials can implement to address common and known risks. The measures include using the .gov top-level domain and HTTPS for all election websites, using multi-factor authentication (MFA) for all election systems, implementing DMARC for email security, and implementing efficient and effective pre- and post-election audits of voting systems. The Subsector will continue to identify security measures and improvements through assessments and promote identified measures to stakeholders.

Subsector partners have contributed to resources that help election officials apply important security considerations to procurement decisions and documents, including a procurement guide created by the CIS. The GCC also released a funding considerations document in 2018 that provided high-level guidance to state and local election officials considering purchases in the wake of additional 2018 HAVA funding—and is in the process of producing a follow-on document related to money in the Fiscal Year 2020 Appropriations Bill. The purpose of these efforts is to provide instruction and ideas on how to build security into election technology procurements, in addition to educating and building confidence in election officials with respect to interacting with cybersecurity and other technology vendors.

Meanwhile, SCC partners have provided guidance for election entities regarding sound practices in cyber hygiene, physical security, pre- and post-election protocols, and chain of custody practices.

The GCC and SCC are also exploring how to leverage the work of security researchers to improve the security posture of election officials and industry providers. Through the EI-SIG, major voting systems manufacturers released a white paper in August 2019 on their voluntary efforts to establish an industry-wide CVD program, followed by a more formal Request for Information (RFI) in September 2019. SCC members have also begun working with DHS's Critical Product Evaluation program to conduct additional security testing on their elections products. Conversations have begun between DHS, the EAC,

EXHIBIT 2

and industry partners to ensure that vulnerabilities discovered via additional testing can be ameliorated within the EAC's certification process in a timely manner. Meanwhile, the GCC is exploring options for a CVD program, potentially through the EI-ISAC.

3.3.3 Resources

Assist Subsector partners in determining priorities, programs, and budgets for securing their entities and assets.

    a. **INVESTMENT** - Develop consistent and sustainable sources of support from governments at the local, state, and federal levels as well as nonprofits and the private sector for election security measures that are appropriately flexible and based on the threat landscape.

    b. **RESEARCH** - Identify resource and knowledge gaps in securing election infrastructure to build tools and programs for Subsector-wide use.

ELECTION SUBSECTOR ACTIVITY	STATUS	COUNCIL
Identify resourcing gaps at the federal, state, and local level and identify existing resources or funding requirements necessary to fill those gaps	**Incomplete** – GCC will establish Research Working Group. Ongoing GCC engagements with the National Conference of State Legislatures (NCSL), the National Association of Counties (NACo), the National Governors Association (NGA), and others (e.g., National Guard) that may influence ongoing funding environments and/or technical capacity building	**GCC**
Engage stakeholders that may influence ongoing funding environments	**Ongoing** – Engagement with NCSL, NACo, NGA, and others	**GCC**
Engage stakeholders who may provide resources other than funding	**Ongoing** – Engagement with the National Association of State Chief Information Officers (NASCIO), NGA, National Guard, and others	**GCC**
Engage with third-party groups that can serve as validators and amplifiers of challenges faced by Subsector stakeholders	**Ongoing** – Engagement with non-profit and academic researchers who amplify challenges and resource needs (both monetary and nonmonetary) faced by election infrastructure stakeholders	**GCC** and **SCC**
Work with stakeholders to develop research agenda for election infrastructure	**Incomplete** –Establish a Research Working Group. GCC and SCC members continue to serve as Subject Matter Experts (SMEs) for ongoing efforts	**GCC** and **SCC**

Investment

The Election Infrastructure Subsector deals with chronic resourcing issues at all levels of government. The designation of elections as critical infrastructure in 2017 has brought state and local election office resourcing to the forefront, particularly among federal appropriators. In March 2018, Congress funded the remaining $380 million, with a five percent match by the states under HAVA, and the EAC worked to disburse funds to all states by August. However, a new provision requiring that states use the money within five years of the President's signature made long-term planning difficult, and the timing of the disbursement meant that SLTT election officials were constrained as to what they could accomplish by the November 2018 election. The one-time nature of this appropriation is also limiting: technology is not a one-time investment, and without sustainable funding, SLTT election officials must budget their share of the funds to ensure that they can afford to maintain the technologies, practices, and trainings that they put into place in 2018 in the future.

In December 2019, Congress added another $425 million in one-time funding, again utilizing the HAVA appropriations formula for equitable distribution of the funds, this time including the Commonwealth of the Northern Mariana Islands for the first time. The EAC took point to distribute the funds. Unlike the 2018 funds, the state match to receive the 2019 funds was 20 percent, an increase over the five percent required in 2018. There is widespread agreement among GCC members that more resources—and, importantly, more sustained resources—will improve election security. Funding shortages affect both state and local election officials, though in different ways.

EXHIBIT 2

The problem of adequate funding is not solely a federal issue, though. Election officials often lack adequate state and local funding for the necessary ongoing procurement and maintenance of election technology. Improving funding levels from state and local appropriators is a priority for SLTT election officials.

State election officials, mostly through NASS and NASED, engage with groups who influence resource environments at the state and local level to highlight resource needs including both stable funding and nonmonetary resources such as technical support, help with risk assessments, and surge support for incident response. The clear national importance of election infrastructure has made engagement with other stakeholder groups, including the NGA, NASCIO, NACo, the NCSL, and others easier, and more important, than ever before. These groups are collaborating with SLTT election officials in varying ways to elevate elections in resource conversations, continuity of operations planning, and disaster preparedness. State and local election officials have also engaged with third-party groups who have served as amplifiers of the resourcing challenges faced by Subsector partners. But until the Federal Government creates sustainable funding, and/or until state and local governments step up to support election infrastructure security in a robust fashion across all election jurisdictions, the funding for appropriate election security will continue to be a problem for election administrators.

Research

Addressing research and development priorities requires Subsector-wide engagement. The GCC and the SCC are working to formalize research and development plans and processes to bring new knowledge, techniques, and capabilities to the Subsector. Collaboration priorities may provide a means for outreach, review of ongoing research and development efforts by the SSA and other federal and state government entities, consideration of gaps in the execution of national research and development priorities, and the opportunity to reach consensus on government and private sector roles and responsibilities. The GCC and SCC intend to establish a Research Working Group to address the funding challenges described above, as well as guide other research as needed. The Working Group will be tasked with identifying the most critical resourcing gaps for the Subsector and identifying existing resources or funding requirements necessary to address those gaps.

Subsector partners recognize the need to be forward-thinking by focusing not only on the assets necessary to administer elections today, but also on elections in the future. Specifically, Subsector partners also plan to work with DHS, NIST, the EAC, and others to develop a research agenda for election infrastructure that will focus on longer term election security past 2020.

EXHIBIT 2

4. NATIONAL PREPAREDNESS AND RESILIENCE STRATEGIES

Preparedness for cyber and physical disruptions in service is a major focus for the Election Infrastructure Subsector. The recognition of conducting elections as a National Critical Function[15] further highlights the importance of preparedness in the Subsector. State and local election officials must continuously deliver election services throughout the jurisdictions they serve, especially during election and voting periods. This means providing real-time or near real-time access to physical and cyber/digital assets supporting elections even when regular delivery mechanisms have failed due to a natural disaster or security incident. Resilience requires restoring regular services after such events and adapting services and delivery mechanisms in the face of new risks. Backups, both physical and technological, and disaster recovery operations are part of the process of restoring delivery mechanisms.

Presidential Policy Directive 8: National Preparedness (PPD-8) affirms that preparation for national emergencies is a shared responsibility of all levels of government and the private and non-profit sectors. It also calls for a National Preparedness System to help align the efforts of all partners.[16] The Subsector contributes to national preparedness by mitigating risks to election systems and assets.

The National Preparedness Goal describes a vision for preparedness nationwide and identifies the core capabilities necessary to achieve that vision across five mission areas: Prevention, Protection, Mitigation, Response, and Recovery.[17] The nature of election infrastructure and the scope of its functions mean preparedness in the Subsector must include activities from each of these mission areas. Efforts to incorporate the national preparedness mission areas translate to more secure and resilient election infrastructure and, therefore, a more secure and resilient national psyche.

Election Infrastructure Subsector National Preparedness Efforts

Election infrastructure resilience efforts include measures designed to prevent, deter, and mitigate threats to election administration; reduce vulnerability to misinformation; minimize the consequences on election outcomes and perception; and enable timely, efficient response and restoration following incidents. Every day across the United States, the Subsector organizes and executes its security and resilience programs and activities in a manner consistent with all five of the national preparedness frameworks that correspond to the five mission areas—National Prevention Framework, National Protection Framework, National Mitigation Framework, National Response Framework, and National Disaster Recovery Framework—in addition to the implementation of the National Incident Management System. The programs and activities that contribute to the security and resilience of the Subsector are diverse and developed collaboratively by federal and SLTT governments, including NASS, NASED, the EAC, the GCC and SCC, and private sector and non-profit partners, along with industry associations and others.

---

[15] Cybersecurity and Infrastructure Security Agency, *National Critical Functions Set*, April 30, 2019, https://www.cisa.gov/sites/default/files/publications/national-critical-functions-set-508.pdf.

[16] Department of Homeland Security, *Presidential Policy Directive/PPD-8: National Preparedness*, accessed June 6, 2019, https://www.dhs.gov/presidential-policy-directive-8-national-preparedness.

[17] Federal Emergency Management Agency, *National Preparedness Goal, Second Edition*, September 2015, https://www.fema.gov/media-library-data/1443799615171-2aae90be55041740f97e8532fc680d40/National_Preparedness_Goal_2nd_Edition.pdf.

EXHIBIT 2

APPENDIX A: COORDINATING COUNCIL MEMBER PROFILES

Election Infrastructure Subsector Government Coordinating Council

The Election Infrastructure Subsector GCC consists of 24 representatives derived from the membership of associations of state and local election officials, plus three Federal Government representatives, as laid out in the Election Infrastructure Subsector GCC Charter.[18] The organizations whose members are represented on this GCC are:

International Association of Government Officials (iGO): The iGO has a very large contingent of election officials from around the Nation and world. The Domestic Election Section of iGO is committed to the security of elections from current threats. Three members on the GCC represent the iGO, though other GCC members may also be iGO members. The Association aims to provide professional training and leadership development through the promotion of networking, technology innovations, educational programs, and legislative monitoring on national issues that affect county recorders, election officials, treasurers, and clerks, to better serve the public.[19]

National Association of Secretaries of State (NASS): In 40 states, the Secretary of State serves as the Chief Election Official, charged with driving state election policy and ensuring compliance with the rules. NASS has eight members on the GCC. Founded in 1904, NASS is the Nation's oldest non-partisan professional organization for public officials. Membership is open to all 50 states, the District of Columbia, and all U.S. Territories. NASS serves as a medium for the exchange of information between states and fosters cooperation in the development of public policy. The Association has key initiatives in the areas of elections and voting, state business services, and state heritage/archives.[20]

National Association of State Election Directors (NASED): The NASED mission is to promote accessible, accurate, and transparent elections in the United States and U.S. Territories. NASED has six positions on the GCC. The Association was formed in 1989 when a group of state election directors and administrators met in Reno, Nevada. The driving issue at that time that spurred the group to organize was the concern that national networks were releasing presidential election results before all polls had closed. HAVA has increased the importance for communication and coordination among state election directors. Though the issues have changed somewhat over the years, the purpose of NASED has remained the same—to serve as an exchange of best practices and ideas.[21]

National Association of Election Officials: The National Association of Election Officials, also known as the Election Center, is a non-profit organization built to promote, preserve, and improve democracy.[22] The Election Center may appoint three local election officials to the GCC. Its members are almost exclusively government employees whose jobs are to serve in voter registration and elections administration. This includes voter registrars, election supervisors, election directors, city clerks/city secretaries, county clerks, county recorders, state legislative staff, state election directors and the Secretary of State for each of the individual states, territories, and the District of Columbia. The Election Center provides its members with an alert service, which informs and updates state, city, and other election and voter registration officials regarding legislation, regulations, court decisions, and U.S. Department of Justice rulings that affect the conduct of voter registration or elections administration. Additionally, the Election Center performs research for such governmental units concerning the similarities and differences in state or local laws, regulations, or practices concerning voter registration and elections administration.[23]

U.S. Department of Homeland Security (DHS): As the designated SSA for the Election Infrastructure Subsector, DHS's primary role is to build trusted partnerships and advance a national unity of effort to strengthen and maintain secure, functioning, and resilient election infrastructure, as laid out in PPD-21. DHS performs this role (as well as a similar role for other critical infrastructure sectors) via CISA, which encompasses a variety of personnel, capabilities, resources, and technical

---

[18] U.S. Department of Homeland Security (DHS), *EIS GCC Charter*, October 18, 2017, https://www.cisa.gov/sites/default/files/publications/govt-facilities-election-infrastructure-subsector-gcc-charter-2017-508.pdf.

[19] International Association of Government Officials (iGO), "About iGO," accessed May 11, 2018, https://iaogo.org/about/.

[20] National Association of Secretaries of State (NASS), "About NASS," accessed May 11, 2018, http://www.nass.org/index.php/about-nass.

[21] National Association of State Election Directors (NASED), "About NASED's History," accessed May 11, 2018, https://www.nased.org/about-nased/.

[22] National Association of Election Officials, "About Us," accessed May 11, 2018, https://www.electioncenter.org/about-us.html.

[23] Orange County Registrar of Voter, "Our People," accessed May 11, 2018, https://www.ocvote.com/about/our-people/.

EXHIBIT 2

expertise that state and local election officials can leverage on a voluntary basis to support the security and resilience of their election infrastructure. Under PPD-21 and the NIPP, DHS provides a venue for a voluntary, structured partnership approach between the government and the private sector for the protection, security, and resilience of critical infrastructure. The Election Infrastructure GCC and SCC are established under this framework.[24]

U.S. Election Assistance Commission (EAC): As the primary partner in the Subsector for DHS, the EAC brings election official support and management experience to the table as this new Subsector stands up. The EAC was established by HAVA. It is an independent, bipartisan commission charged with developing guidance to meet HAVA requirements, adopting voluntary voting system guidelines, and serving as a national clearinghouse of information on election administration. The EAC also accredits testing laboratories, certifies voting systems, and audits the use of HAVA funds. Other responsibilities include maintaining the national mail voter registration form developed in accordance with NVRA. HAVA established the Standards Board and the Board of Advisors to advise the EAC. The law also established the Technical Guidelines Development Committee to assist the EAC in the development of voluntary voting system guidelines. The four EAC commissioners are appointed by the President and confirmed by the U.S. Senate. The EAC is required to submit an annual report to Congress as well as testify periodically about HAVA progress and related issues. The Commission also holds public meetings and hearings to inform the public about its progress and activities.[25]

EAC Board of Advisors: The EAC Board of Advisors is composed of 35 representatives from the NGA; NCSL; NASS; NASED; NACo; iGO; Election Center; International Association of Clerks, Recorders, Election Officials, and Treasurers; U.S. Commission on Civil Rights; and Architectural and Transportation Barriers Compliance Board. Other members include representatives from the U.S. Department of Justice, Office of Public Integrity, and the Civil Rights Division; the director of the U.S. Department of Defense's FVAP; four professionals from the field of science and technology, one each appointed by the Speaker and the Minority Leader of the U.S. House of Representatives and the Majority and Minority leaders of the U.S. Senate; and eight members representing voter interests, with the chairs and the ranking minority members of the U.S. House of Representatives Committee on House Administration and the U.S. Senate Committee on Rules and Administration each appointing two members.

Following the passage of HAVA, the National Association of County Recorders, Election Officials and Clerks and the International Association of Clerks, Recorders, Election Officials, and Treasurers merged to form the International Association of Government Officials. It advises the EAC through the review of the voluntary voting systems guidelines (VVSG) described in HAVA. This includes the review of the voluntary guidance and best practices recommendations therein. It functions solely as an advisory body under the provisions of the Federal Advisory Committee Act.[26]

EAC Standards Board: The Standards Board is a 110-member body designated by HAVA to assist the EAC in carrying out its mandates under the law. The Board consists of 55 state election officials selected by their respective Chief Election Officials, and 55 local election officials selected through a process supervised by the Chief Election Officials. Similar to the EAC Board of Advisors, the Standards Board advises the EAC through review of the VVSG, voluntary guidance, and best practices under HAVA.[27]

Election Infrastructure Subsector Coordinating Council

The Election Infrastructure SCC is a self-organized, self-run, and self-governed body of organizations representing the private sector components of election infrastructure. Members of the SCC include companies, organizations, or components thereof whose services, systems, products, or technology are used by (or on behalf of) state or local governments in the administration of U.S. elections.

To qualify for membership, the SCC requires organizations to demonstrate working relationships with federal, state, or local election officials, which may include verifiable registration or accreditation with the EAC and/or relevant contractual relationships with SLTT government election offices.[28]

---

[24] U.S. Department of Homeland Security (DHS), "About DHS," accessed May 11, 2018, https://www.dhs.gov/about-dhs.

[25] U.S. Election Assistance Commission (EAC), "About U.S. EAC," accessed May, 11, 2018, https://www.eac.gov/about-the-useac/.

[26] U.S. Election Assistance Commission (EAC), "Advisory Boards: Board of Advisors," accessed May 11, 2018, https://www.eac.gov/about/board-of-advisors/.

[27] U.S. Election Assistance Commission (EAC), "Advisory Boards: Standards Board," accessed May 11, 2018, https://www.eac.gov/about/standards-board/.

[28] U.S. Department of Homeland Security (DHS), *EISCC Charter*, February 15, 2018, https://www.cisa.gov/government-facilities-election-infrastructure-charters-and-membership.

EXHIBIT 2

APPENDIX B. GLOSSARY OF TERMS

This appendix includes definitions of the terms used in the SSP and adapted from the NIPP. For a broader glossary of election infrastructure terms, please refer to the EAC's *Glossary of Key Election Terminology*.[29]

All Hazards: A term that encompasses threats or incidents, natural or man-made, that warrant action to protect life, property, the environment, and public health or safety and minimize disruptions of government, social, or economic activities.

Consequence: The effect of an event, incident, or occurrence, including the number of deaths, injuries, and other human health impacts, along with the economic impacts, both direct and indirect, and other negative outcomes to society.

Critical Infrastructure: Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems would have a debilitating impact on security, national economic security, national public health or safety, or any combination thereof.

Critical Infrastructure Sectors: A logical collection of assets, systems, or networks that provide a common function to the economy, government, or society; PPD-21 identifies 16 critical infrastructure sectors.

Cyber: Describes electronic technologies or components of systems that operate in an internet-connected state, or those that can be connected to the internet.

Digital: Describes electronic technologies or components of systems that operate without necessarily being connected to the internet.

Election Infrastructure Subsector Partners: The GCC, SCC, and the respective stakeholder groups they represent in efforts to ensure the security and resilience of the Election Infrastructure Subsector.

Election Systems: Includes infrastructure to manage voter registration, planning and execution of elections, counting and reporting of election results, and other software and hardware used by election officials.

Federal Virtual Training Environment (FedVTE): A free, online, and on-demand cybersecurity training system for federal/SLTT government personnel and veterans. Managed by DHS with support from the U.S. Department of Defense's Defense Information Systems Agency, FedVTE offers more than 800 hours of training on topics such as ethical hacking and surveillance, risk management, and malware analysis. Courses range from beginner to advanced levels. Training is accessible from any internet-enabled computer.

Government Coordinating Council (GCC): Consists of representatives from across various levels of government (including federal and SLTT), as appropriate to the operating landscape of each individual sector. These councils enable inter-agency, intergovernmental, and cross-jurisdictional coordination within and across sectors and partner with SCCs on public-private efforts.

Homeland Security Information Network–Election Infrastructure Subsector (HSIN-EIS): A trusted network to share Sensitive but Unclassified information with federal, state, local, territorial, international, and private sector partners.

Lifeline Function: A function that is essential to the operation of most critical infrastructure sectors. The NIPP 2013 identifies communications, energy, transportation, and water as lifeline functions. Critical infrastructure partners should identify essential functions and resources that impact their businesses and communities.

Private Sector Clearance Program: A program administered by DHS designed to facilitate access to security clearances for private sector officials involved in the infrastructure protection mission.

---

[29] U.S. Election Assistance Commission (EAC), "Election Officials: Glossaries of Election Terminology," accessed May 8, 2018, https://www.eac.gov/glossary?pg=1.

EXHIBIT 2

Risk: The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.

Sector-Specific Agency (SSA): A federal department or agency designated by PPD-21 with responsibility for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment.

Subsector Coordinating Council (SCC): SCCs are self-organized, self-run, and self-governed private sector councils consisting of owners and operators and their representatives, which interact on a wide range of sector-specific strategies, policies, activities, and issues. SCCs serve as principal collaboration points between the government and private sector owners and operators for critical infrastructure security and resilience policy coordination and planning and a range of related sector-specific activities. For election infrastructure, the Council includes the owners and operators for the Subsector.

Subsector Partners: See "Election Infrastructure Subsector Partners."

Threat: A natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.

Vulnerability: A physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.

EXHIBIT 2

APPENDIX C. ACRONYMS AND ABBREVIATIONS

Acronym	Definition
2FA	Two-Factor Authentication
BMD	Ballot Marking Devices
CIIA	Critical Infrastructure Information Act of 2002
CIO	Chief Information Officer
CIPAC	Critical Infrastructure Partnership Advisory Council
CISA	Cybersecurity and Infrastructure Security Agency
CIS	Center for Internet Security
CSA	Cyber Security Advisor
CTCL	Center for Technology and Civic Life
CVD	Coordinated vulnerability disclosure
DHS	U.S. Department of Homeland Security
DMARC	Domain Based Message Authentication, Reporting and Conformance
DMV	Department of Motor Vehicles
DNI	Office of the Director of National Intelligence
DRE	Direct Recording Electronic
EAC	Election Assistance Commission
EC-Council	International Council of E-Commerce Consultants
EI-ISAC	Election Infrastructure Information Sharing and Analysis Center
EMP	Electro-magnetic pulse
EO	Executive Order
FBI	Federal Bureau of Investigation
FedVTE	Federal Virtual Training Environment
FEMA	Federal Emergency Management Agency
FVAP	Federal Voting Assistance Program
GCC	Government Coordinating Council
GIS	Geographic Information System
HAVA	Help America Vote Act
HSIN-EIS	Homeland Security Information Network-Election Infrastructure Subsector
HTTPS	Hypertext Transfer Protocol Secure
I&A	DHS Office of Intelligence and Analysis
iGO	International Association of Government Officials
ISAC	Information Sharing and Analysis Center
IT	Information technology

Acronym	Definition
MFA	Multi-factor authentication
MS-ISAC	Multi-State Information Sharing and Analysis Center
NACo	National Association of Counties
NASCIO	National Association of State Chief Information Officers
NASED	National Association of State Election Directors
NASS	National Association of Secretaries of State
NCCIC	National Cybersecurity and Communications Integration Center
NCI	National Council of Information Sharing and Analysis Centers (ISACs)
NCOA	National Change of Address
NCSL	National Conference of State Legislatures
NGA	National Governors Association
NIPP 2013	National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience
NIST	National Institute of Standards and Technology
NGO	Nongovernmental organization
NRMC	National Risk Management Center
NVRA	National Voter Registration Act
PPD-8	Presidential Policy Directive 8: National Preparedness
PPD-21	Presidential Policy Directive 21: Critical Infrastructure Security and Resilience
PSA	Protective Security Advisor
R&D	Research and Development
RC3	Regional Consortium Coordinating Council
RFI	Request for information
SCC	Subsector Coordinating Council
SIG	Special interest group
SLTT	State, local, tribal, and territorial
SME	Subject matter expert
SSA	Sector-Specific Agency or Subsector-Specific Agency
SSP	Subsector-Specific Plan
USPS	United States Postal Service
VVSG	Voluntary voting systems guidelines

EXHIBIT 2

APPENDIX D. ELECTION INFRASTRUCTURE AUTHORITIES

This appendix provides a brief description of the major authorities and resources that form the basis for the establishment of the Election Infrastructure Subsector security and resilience partnership.

Critical Infrastructure Authorities

Homeland Security Act of 2002, as amended: The Homeland Security Act establishes specific critical infrastructure protection roles and responsibilities for DHS which include:[30]

- developing a comprehensive national plan for securing the critical infrastructure of the United States;

- providing crisis management in response to attacks on critical information systems;

- providing technical assistance to the private sector and other government entities on emergency recovery plans for failures of critical information systems; and

- coordinating with federal agencies to provide specific warning information and advice about appropriate protective measures and countermeasures to state, local, and nongovernment entities.

Critical Infrastructure Information Act of 2002 (CIIA): The CIIA establishes protections for critical infrastructure information that is voluntarily shared with DHS for use regarding the security of critical infrastructure and protected systems. CIIA includes measures to ensure against DHS disclosure of protected critical infrastructure information to encourage private and public sector entities to voluntarily share their critical infrastructure information with DHS.[31]

Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (PPD-21): This PPD directs the executive branch to develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time; understand the cascading consequences of infrastructure failures; evaluate and mature the public-private partnership; update the NIPP; and develop a comprehensive research and development plan.[32]

National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience (NIPP 2013): The NIPP 2013 is informed by significant evolution in the critical infrastructure risk, policy, and operating environments, as well as experience gained and lessons learned from the previous 2009 NIPP. The 2013 plan builds upon prior NIPPs by emphasizing the complementary goals of security and resilience for critical infrastructure. To achieve these goals, cyber and physical security and the resilience of critical infrastructure assets, systems, and networks are integrated into an enterprise approach to risk management. The NIPP 2013 guides the national efforts to manage risk to the Nation's critical infrastructure.[33]

Executive Order (EO) 13636 – Improving Critical Infrastructure Cybersecurity: This EO directs the executive branch to develop a technology-neutral, voluntary cybersecurity framework; promote and incentivize the adoption of cybersecurity practices; increase the volume, timeliness, and quality of threat information sharing; incorporate strong privacy and civil liberties protection into every critical infrastructure security initiative; and explore the use of existing regulations to promote cybersecurity.[34]

---

[30] *Homeland Security Act of 2002, as amended. Pub. L.* 107-296, 116 Stat. 2135, (2002).

[31] *Critical Infrastructure Information Act (CIIA),* 6 U.S.C. 671-674.

[32] The White House, *Presidential Policy Directive: Critical Infrastructure Security and Resilience (PPD-2013),* February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[33] U.S. Department of Homeland Security (DHS), *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience (NIPP 2013),* 2013, https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf.

[34] The White House, *Executive Order 13636 – Improving Critical Infrastructure Cybersecurity,* February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

EXHIBIT 2

Designation of Election Infrastructure as a Subsector of the Government Facilities Critical Infrastructure Sector: The former DHS Secretary issued a memorandum on January 6, 2017, to officially designate the Election Infrastructure Subsector. The memorandum defines the physical assets and information and communication technologies that constitute the elements of election infrastructure that are considered critical infrastructure. It also directs NPPD (National Protection and Programs Directorate, now CISA) to establish an SSA management office to support the Subsector's institutionalization under the NIPP.[35]

Other Federal Authorities

Executive Order 13848: Following the revelation that foreign adversaries had attempted to interfere in the 2016 election, the U.S. Government took steps to implement policies designed to deter malicious actors from attempting to interfere in future elections.

Executive Order 13848, Imposing Certain Sanctions in the Event of Interference in U.S. Elections, establishes a process for the U.S. Government to implement economic sanctions against the perpetrators of election interference and the entities who support them. The EO empowers the Secretary of the Treasury, in consultation with the Attorney General, Secretary of State, and Secretary of Homeland Security, to block malicious actors' property, restrict their access to financial institutions, and "other measures authorized by law."

Per the EO: "[T]he term 'foreign interference,' with respect to an election, includes any covert, fraudulent, deceptive, or unlawful actions or attempted actions of a foreign government, or of any person acting as an agent of or on behalf of a foreign government, undertaken with the purpose or effect of influencing, undermining confidence in, or altering the result or reported result of, the election, or undermining public confidence in election processes or institutions."[36]

National Defense Authorization Act: The 2020 National Defense Authorization Act for Fiscal Year 2020 includes numerous provisions related to election security and establishes several new requirements for federal agencies and departments. Specifically, it requires DHS to:

- with the DNI and FBI, post any counterintelligence threats to political campaigns for federal office on the internet, provide update briefings to Congress, and conduct a post-election assessment;[37]

- report to Congress any foreign government cyberattacks against the U.S. 2016 election;

- with the Intelligence Community, conduct an assessment of U.S. election systems vulnerabilities at least one year prior to any federal election and submit a report to Congress on such; and

- with the DNI and FBI, brief Congress following any significant foreign cyber intrusions or active measures campaigns directed against the U.S. election system.[38]

---

[35] U.S. Department of Homeland Security (DHS), "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector," press release, January 6, 2017, https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

[36] The White House, *Executive Order 13848 — Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election*, September 12, 2018, https://www.whitehouse.gov/presidential-actions/executive-order-imposing-certain-sanctions-event-foreign-interference-united-states-election/.

[37] *National Defense Authorization Act for Fiscal Year 2020*, Pub. L. 116-92, § 5304, (2019).

[38] *National Defense Authorization Act for Fiscal Year 2020*, Pub. L. 116-92, § 6503-6507, (2019).